

Strengthening your cybersecurity management with our **expert consulting services**

Enhance the effectiveness of your cybersecurity management by ensuring compliance and adopting industry best practices.

Technology is advancing at an unprecedented rate, making cybersecurity more complex and sophisticated. With the growing number of connected devices, cloud computing, and remote work, businesses face rapidly expanding cybersecurity responsibilities. Cybersecurity threats, including malware, phishing attacks, ransomware, and social engineering, can result in significant financial losses, reputational damage, and legal liabilities. Managing cybersecurity in today's digital landscape requires expertise in risk assessment, compliance management, incident response, and employee education.

As businesses rely more heavily on technology, they become increasingly vulnerable to cyber attacks. Each threat requires a unique approach to mitigate, and staying ahead of emerging threats can be challenging. Compliance with regulations and standards such as GDPR, NIS2, NIST and ISO 27001 is becoming more stringent, and companies must comply to avoid penalties and legal liabilities. Effective cybersecurity management is more critical than ever!

At our cybersecurity consulting practice, we understand the challenges that businesses face in managing cybersecurity. We offer a range of services to help companies achieve and maintain compliance with cybersecurity regulations and standards, assess and manage cybersecurity risks, and respond effectively to cybersecurity incidents. Our team of experts holds relevant certifications and has extensive experience working with large and medium-sized B2B clients across various sectors.

In conclusion, managing cybersecurity is a complex and constantly evolving task that requires expertise in a wide range of areas.

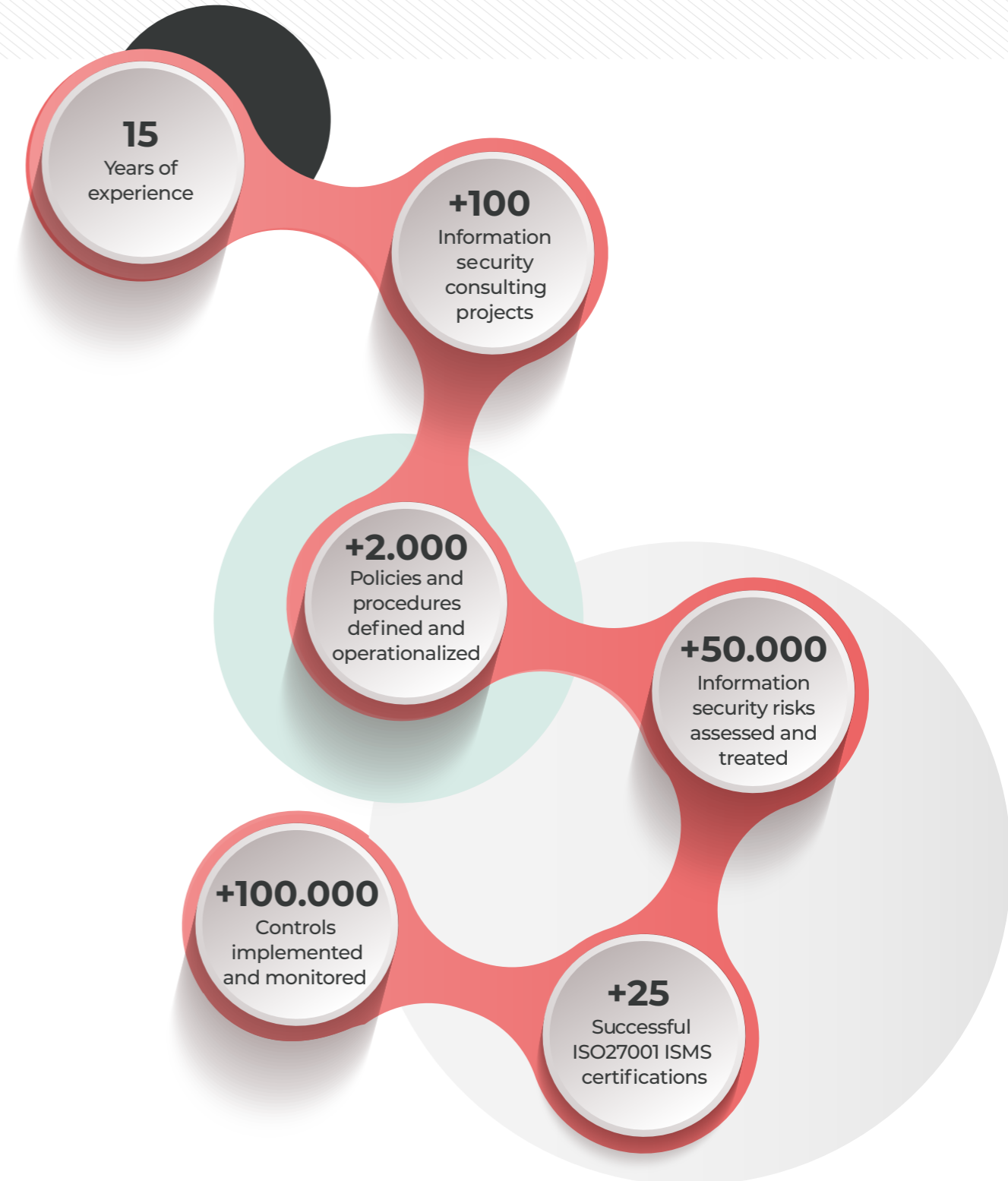
At our cybersecurity consulting practice, we can provide the expertise and support that businesses need to effectively manage their cybersecurity risks and protect against emerging threats.

Our experience

For over 15 years, our cybersecurity consulting practice has been helping businesses across a wide range of sectors proactively manage their cybersecurity risks. We have helped dozens of companies assess and mitigate thousands of risks, and we have drafted hundreds of policies and procedures to ensure compliance with cybersecurity regulations and standards.

Our team of cybersecurity experts has extensive experience working with large and medium-sized B2B clients, and we hold relevant certifications such as ISO 27001 LA/LI, CISA, CISM, CRISC, CDPSE and others. We have a deep understanding of the evolving cybersecurity landscape and stay up-to-date with the latest threats, trends, and regulations.

We take a customised approach to cybersecurity consulting, working closely with our clients to understand their unique needs and develop tailored solutions that mitigate risks and enhance their cybersecurity posture. Our proven track record of success speaks for itself, and we are committed to providing the highest quality cybersecurity consulting services to our clients.



Our main compliance frameworks

In our pursuit of effectiveness and efficiency in cybersecurity, we avoid reinventing the wheel. Instead, we harness the power of established frameworks while skillfully adapting them to meet the unique needs of each client. This approach allows us to provide customised solutions while leveraging tried-and-true methods that have proven their worth in the field of cybersecurity.

▶ **ISO 27001 / ISO27701:** ISO 27001 / ISO27701 are internationally recognised standards that outline best practices for information security, cybersecurity and privacy protection. They provide a systematic approach to managing sensitive company information and mitigating information security, cybersecurity and privacy risks. Achieving ISO 27001 and ISO27701 certifications demonstrates an organisation's commitment to information security, cybersecurity and privacy protection and can help build trust with clients, partners, and stakeholders.

▶ **NIS2:** The Network and Information Systems Directive (NIS2) is an EU-wide legislation that requires organisations in critical infrastructure sectors to implement robust cybersecurity measures, report security incidents, and maintain compliance with strict regulations and standards. Achieving compliance with NIS2 is critical for organisations in these sectors, as failure to comply can result in significant financial penalties and reputational damage.

▶ **NIST CSF:** The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a framework for managing and reducing cybersecurity risk. It was developed by NIST in response to Executive Order 13636, which called for the development of a framework to improve the cybersecurity of critical infrastructure in the United States.

Overall, the NIST CSF is designed to be flexible, customisable, and scalable, and can be used by organisations of all sizes and in all sectors to improve their cybersecurity posture. By using the Framework, organisations can better manage and reduce their cybersecurity risks and improve their overall resilience to cyber threats.

▶ **GDPR:** The General Data Protection Regulation (GDPR) is a regulation that governs the protection of personal data of individuals within the European Union (EU) and the European Economic Area (EEA). It came into effect on May 25, 2018, and replaced the EU's previous data protection regulation.

Overall, the GDPR is designed to strengthen individuals' rights over their personal data and increase transparency and accountability around data processing. It has significant implications for organisations that process personal data, both within and outside the EU and EEA.

Our common compliance management process

Laws, Standards and Regulations

Management of compliance nodes (requirements/controls/other type of obligations) regarding laws, standards and regulations.

Workflows

Modelling and operationalisation of any required workflow.

Risk Management

Definition operationalisation of risk management processes.



Documented information

Management of **Policies, Procedures, Rules** and other documented information life cycle.

Activities

Control of **management and operational activities** related with documented information and any other relevant activities.

Assessments

Execution of **compliance self-assessments** and any **third-parties compliance assessments**.

In addition to the components of the compliance management process presented, there is one more component that is transversal to all of them and that allows the management, control and measurement of effectiveness of all the activities carried out. This component combines information widgets in the appropriate operation and management dashboards for each organisation.

Our Services

Our cybersecurity consulting practice offers a range of services to help clients achieve and maintain compliance with ISO 27001 and NIS2, two critical cybersecurity standards.


Our services include:

- ▶ **Cybersecurity strategy consulting:** We work with clients to develop comprehensive cybersecurity strategies that align with their business objectives and address their unique risks and challenges.
- ▶ **Risk assessment and management:** We help clients identify and assess their cybersecurity risks, develop risk management plans, and implement risk mitigation strategies to protect against potential threats.
- ▶ **Compliance management:** We assist clients in understanding and complying with the complex regulations and standards set forth in ISO 27001/ISO 27701, NIS2, NIST CSF, GDPR, and other cybersecurity standards, helping them develop the policies and procedures necessary to achieve compliance.
- ▶ **Gap analysis:** We conduct comprehensive gap analyses to identify areas where clients may fall short of ISO 27001/ISO 27701, NIS2, NIST CSF, GDPR, and other cybersecurity standards compliance, and we provide recommendations and solutions to address those gaps.
- ▶ **Implementation and certification support:** We provide support throughout the entire ISO 27001/ISO 27701, NIS2, NIST CSF, GDPR, and other cybersecurity standards implementation process, from initial planning to final certification. Our team can guide clients through the process of achieving certification and maintaining compliance.
- ▶ **Process and procedure documentation:** We document processes and procedures for clients to ensure that they have a comprehensive understanding of their cybersecurity management practices and are equipped to identify and mitigate potential threats.
- ▶ **Record keeping:** We assist clients in establishing and maintaining proper record keeping practices to ensure compliance with relevant regulations and standards.
- ▶ **Training and awareness:** We offer customised training and awareness programs to help clients educate their employees on cybersecurity best practices and ensure that they are equipped to identify and mitigate potential threats.

Our managed services approach

KEEP-IT-MANAGED-24

In addition to our traditional consulting services, we also offer a managed services approach to cybersecurity management through our KEEP-IT-MANAGED-24 service. This approach provides clients with ongoing support and guidance to proactively manage cybersecurity and privacy risks and maintain compliance with relevant regulations and standards. Aligned with industry best practices and an organisation's strategic objectives, our service ensures that all components of information security management are addressed in a holistic and systematic manner.

	Abordagem tradicional	Keep IT Managed 24 
Consulting Services	✓	✓
Continued Service	✗	✓
Model adjustable to organisational dynamics	✗	✓
Information Security Management Support Platform	✗	✓
Resource allocation tailored to the dynamic and needs of the organisation	✗	✓
Monitoring the continued evolution of maturity	✗	✓
Redefinition of Goals throughout the service	✗	✓
Response to the organisation's dynamic activities and requirements in the context of Information Security Management	✗	✓
Remote Service Provision whenever applicable for efficiency purposes	✗	✓

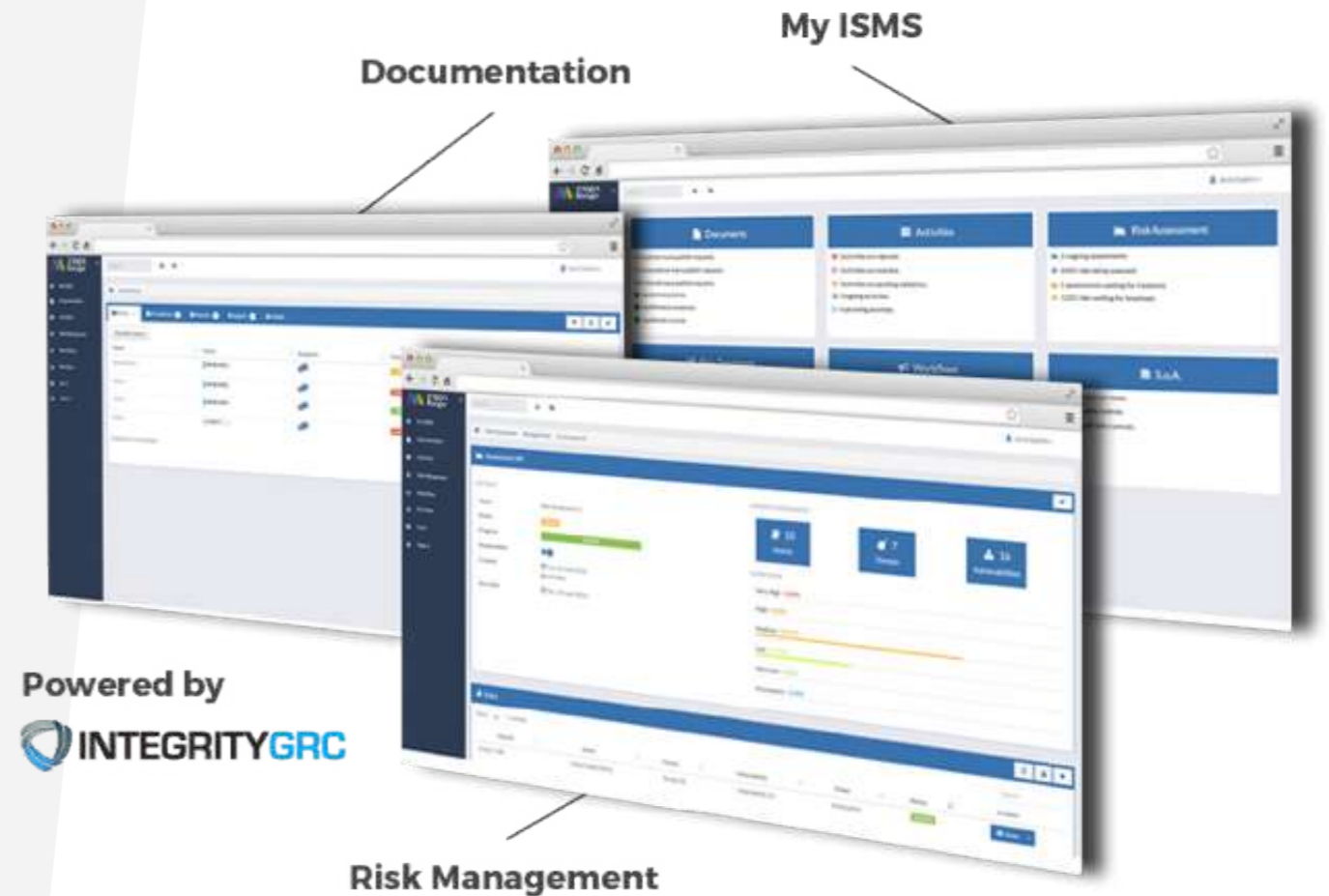
What our clients are saying about us

-  A continuous, proactive approach to managing your organisation's information security, with ongoing support from our expert consultants.
-  Customised solutions tailored to your specific needs and objectives, ensuring that your organisation's security posture is always optimized.
-  A comprehensive and holistic approach that covers all aspects of information security management, including risk assessment, compliance management, and incident response.
-  Access to our proprietary IntegrityGRC platform, which provides a powerful toolset for managing information security risks and maintaining compliance with industry regulations and standards.
-  Regular reporting and feedback, including detailed analysis of potential vulnerabilities and recommendations for remediation.
-  A cost-effective managed services approach, providing long-term security benefits and peace of mind for your organisation.

Boosting our consulting services with **IntegrityGRC**

IntegrityGRC, our proprietary Governance, Risk, and Compliance tool, serves as a force multiplier for our consulting services, enabling our expert consultants to work more efficiently and effectively with our clients, providing deeper insights and more targeted recommendations, and ultimately delivering greater value and outcomes.

On the other hand, clients will benefit from an actionable cybersecurity management system rather than simply a theoretical one. IntegrityGRC provides a practical and customisable solution that allows organisations to efficiently manage their cybersecurity risks and compliance requirements.



Description of Project Team

The technical responsibility for the execution of these consultancy services is that of our specialised consultants, with more than 15 years of experience, with international certifications relevant to the scope in question. In particular:

- CISA (Certified Information Systems Auditor);
- CISM (Certified Information Security Manager);
- CRISC (Certified in Risk and Information Systems Control);
- ISO 27001 Lead Auditor;
- CISSP (Certified Information Systems Security Professional);
- CISSP-ISSMP (Information Systems Security Management Professional);
- OSCP (Offensive Security Certified Professional);
- GPEN (GIAC Penetration Tester);
- eWPTX (eLearnSecurity Web application Penetration Tester eXtreme);
- OSWE (Offensive Security Web Expert);
- PCI QSA (Qualified Security Assessor);
- MSc Information Security;
- PG Information Security.

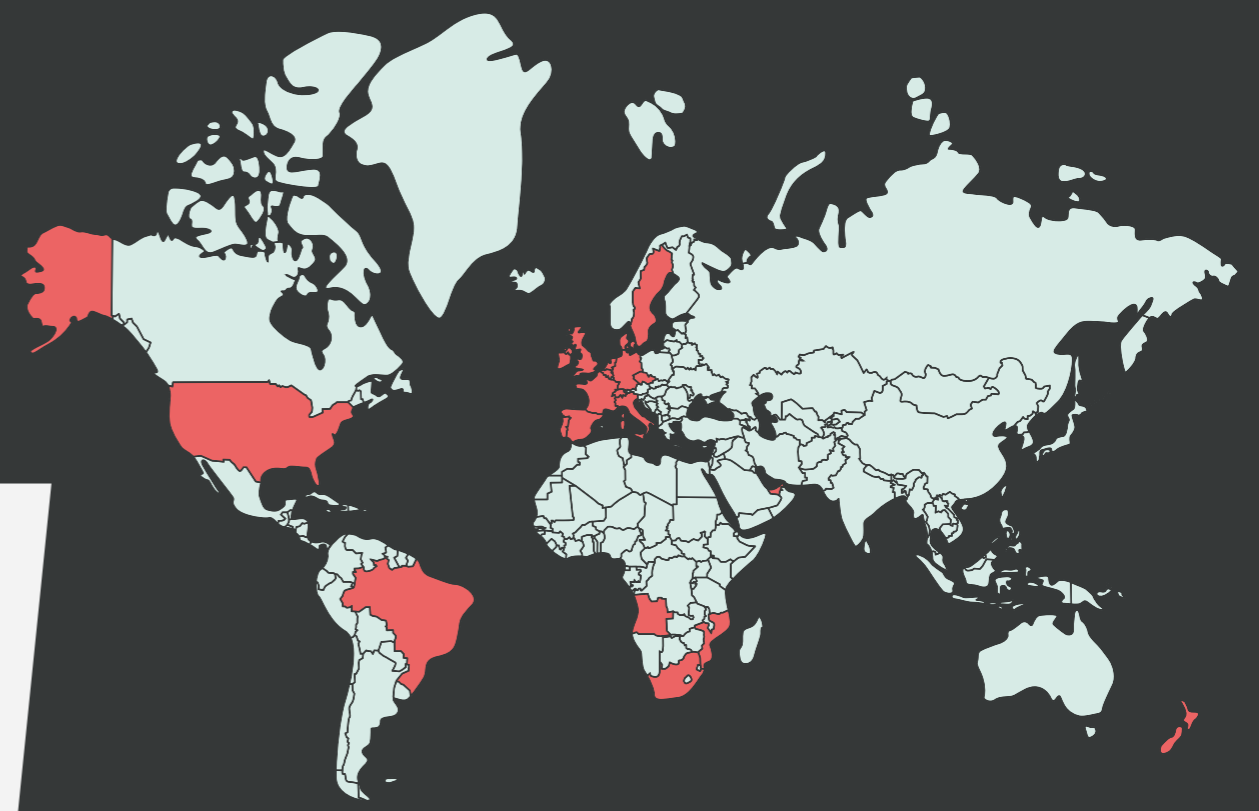
In addition, our consultants are also experienced in various standards and technologies, such as:

- CobIT
- ISO/IEC 19011:2002
- ISACA Auditing Standards and Guidelines
- NISO/IEC 20000
- ISO/IEC 22301
- IST SP-800 Series

Technology : Microsoft, Linux, Cisco, CheckPoint, NetScreen, Nokia, Radware, Packeteer, RSA, McAfee NSP, Symantec CSP (HIDS), Lumension, ClearSwift, among others. .

Certifications & clients

Backed by a diverse portfolio of global clients and a wide range of certifications, including CREST, ISO 27001, ISO 27701, ISO 9001 and PCI QSA, Devoteam Cyber Trust is the premier choice for organisations seeking the highest level of expertise in offensive security services.



ISO 27001 (2012)



CREST (2014)



ISO 9001 (2014)



PNSC (2017)



PCI (2020)



Bancontact (2021)



ISO 27701 (2023)



With HQ in Lisbon, we provide services to a wide **number of large and medium-sized companies**, both at a national and international level.

Know the Benefits

- Comprehensive risk assessment and management, identifying and mitigating cybersecurity risks before they can be exploited by attackers.
- Customised solutions tailored to the unique needs and risks of each client, enhancing their security posture and reducing the likelihood and impact of successful attacks.
- Compliance management, helping clients understand and comply with relevant regulations and standards, such as ISO 27001 /ISO 27701, GDPR, NIS2, NIST CSF and other cybersecurity standards.
- Improved overall cybersecurity management, with a deeper understanding of cybersecurity risks and vulnerabilities, and a proactive approach to risk mitigation.
- Enhanced risk management, with ongoing monitoring and reporting to identify and address emerging cybersecurity risks.
- Cost-effective use of resources and budgets, with a focus on targeted risk assessment and management, and prioritisation of cybersecurity investments.
- Continuous training and awareness programs, helping clients educate their employees on cybersecurity best practices and equip them to identify and mitigate potential threats.
- Trusted expertise, providing clients with the confidence and trust they need to succeed in today's digital landscape.



Case Studies

Implementation and Compliance with ISO 27001

Type of Client: Energy // Over 10.000 employees

Challenge: Our cybersecurity consulting practice was engaged by a large energy company to help them achieve ISO 27001 certification. We developed a comprehensive risk management plan and implemented policies and procedures to mitigate cybersecurity risks and ensure compliance with relevant regulations and standards. After achieving certification, we continued to provide ongoing support through our KEEP-IT-MANAGED-24 service to help the client maintain compliance and proactively manage their cybersecurity risks.

Assessment and Compliance with NIST CSF

Type of Client: Technology // 10 Countries // Over 10.000 employees

Challenge: Our cybersecurity consulting practice was engaged by a technology company with offices in over 10 countries, each of which operated as an independent entity. The client needed to identify and address potential cybersecurity gaps across their global network, and we recommended a gap analysis using the NIST Cybersecurity Framework (CSF). Our assessment provided valuable insights into the client's cybersecurity posture and identified areas for improvement.

What our clients are saying about us

“

The project is a success, the team has loads of technical expertise, they performed above expectations.



“

This is a win-win service and the report level is amazing.



“

It's very easy and reliable to work with Devoteam Cyber Trust



Why engage with **Devoteam Cyber Trust**

- ▶ Deep expertise and experience in cybersecurity consulting with over 15 years of industry-leading experience.
- ▶ A team of highly certified and experienced security professionals, including ISO 27001, NIS2, and GDPR experts, who provide customised solutions to meet the unique needs and goals of each organisation.
- ▶ Comprehensive coverage and flexibility, with a wide range of consulting services and methodologies tailored to the specific cybersecurity risks and challenges facing your organisation.
- ▶ A commitment to quality and excellence, with a focus on delivering the highest levels of service and customer satisfaction.
- ▶ Access to advanced technology and tools, including our proprietary IntegrityGRC tool, to help clients manage their governance, risk, and compliance requirements.
- ▶ Compliance with industry standards and regulations, including ISO 27001, NIS2, GDPR, and other relevant guidelines and frameworks, to help clients mitigate cybersecurity risks and avoid penalties and legal liabilities.
- ▶ A focus on long-term partnerships and ongoing support, with continuous monitoring and reporting providing ongoing feedback and risk management capabilities.
- ▶ A global footprint and reputation, with clients in over 20 countries and a proven track record of delivering effective and high-quality cybersecurity consulting services.



Devoteam Cyber Trust is the right partner to support your organisation in this intense and evolving threat landscape, with best-in-class Offensive Security Services.

This is why dozens of medium-large clients from over 20 countries worldwide trust our services.

We are happy to share **our experience** and help you improve your **cybersecurity practice**.

Balanced risk management requires a solid strategy.

Talk to us.

Contact us



✉ info@integrity.pt

Present in **18 countries in the EMEA region**

www.integrity.pt





www.integrity.pt

www.devoteam.com/expertise/cyber-trust

Devoteam Cyber Trust is the Cybersecurity specialist arm of the Devoteam Group. With our 800+ experts located across EMEA, we aim to establish cybersecurity as an enabler of business success rather than a gatekeeper. We leverage an end-to-end approach to Cyber Resilience, Applied Security, and Managed Security services to secure the tech journey of large and medium-sized companies from all sectors and industries.

Since 2009, previously known as INTEGRITY, our team based in Portugal is specialised in providing cutting-edge Managed Security Services that combine its expertise and proprietary technology to consistently and effectively reduce the cyber risk of our clients. The comprehensive service range includes Persistent intrusion Testing, ISO 27001, PCI-DSS, GRC Consulting and Solutions, and Third-Party Risk Management, ISO 27001 (Information Security), ISO 27701 (Privacy Information Management) and ISO 9001 (Quality) certified, PCI-QSA, and member of CREST and CIS - Centre for Internet Security, we provide services to a considerable number of clients, operating in more than 20 countries.



www.devoteam.com

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity.

By combining creativity, tech and data insights, we empower our customers to transform their business and unlock the future.

With 25 years' experience and 10,000 employees across Europe, the Middle East and Africa, Devoteam promotes responsible tech for people and works to create better change.

Creative tech for Better Change